June 2001
New England Region

FTS Insider

GSA Federal Technology Service
"Tomorrow's Technology Today"

Welcome to the New England Region FTS Insider

-Summer 2001-

June 2001 National Security Awareness Month

The FTS Commissioner, Sandy Bates, has designated the month of June 2001, ***Information Security Awareness Month.***

A few comments by Ms. Bates:

"As you know, information security (IS) and critical infrastructure protection (CIP) are important topics for the federal IT community and all federal employees. IS-related legislative and regulatory mandates, as well as the increased vulnerability that has accompanied increased use of the Internet, all pose tough challenges for government agencies.

To demonstrate the FTS commitment to helping government meet IS challenges successfully, I have designated June 2001 as FTS Information Security Awareness Month. While Information Security is an important aspect of our business all the time, I am asking all FTS personnel to make a special effort during this month to discuss our IS solutions with all potential and existing customers. I have also asked the Customer Action Teams (CATs) to specifically target their accounts with the goal of [re]selling IS solutions.

FTS is a demonstrated leader in the federal IS community, and offers world-class IS solutions through our Client Support Centers as well as our FTS contracts. In addition, the Center for Information Security Services here in Central Office -- the FTS center of expertise for IS solutions -- is available to support all FTS business lines, programs, and regions in meeting customer needs.

Our goal is to increase awareness of FTS Information Security expertise, products, and service offerings. Increasing agencies' awareness of what FTS has to offer in this area will not only add value for our customers, but it will very likely lead to an increase in FTS sales."

Sandy Bates, Commissioner, FTS

The Following is an excerpt from the FTS Web Page posted this month:

When you think of Cyber Security, Information Assurance, and Critical Infrastructure Protection, remember FTS as your solutions provider. We're a neutral government source ready to partner with you in navigating through the technology requirements and acquisition red tape. With expertise from the FTS Center for Information Security Services (CISS) and Client Support Centers located around the country, the GSA Federal Technology Service is making it easier for civilian agencies and the military to obtain those much needed information assurance and critical infrastructure protection solutions. Presidential Decision Directive 63 (PDD 63), Office of Management and Budget (OMB) guidance, and last year's Government Information Security Reform Act (GISRA) make it imperative that Federal agencies plan, update, and implement security programs that keep pace with information technology innovations.

Congress is looking for—and the American people expect—a more accessible government. The goal is to serve citizens on-line, directly and quickly in a secure, private environment. Working with Federal Agencies and world-class Industry Partners, FTS is leading the way with programs for digital signatures, smart cards, and protection from cyber-attacks. Whether it's identifying critical assets, conducting vulnerability assessments and penetration tests, establishing information assurance best practices, or implementing infrastructure protection plans, FTS technology and acquisition professionals are ready to develop solutions to meet all your information security needs.
Key Federal Government Information Security and Information Assurance Requirements and Regulations
To learn more about 21st Century Information Security Solutions from the GSA Federal Technology Service, contact your local FTS Customer Support Representative or the FTS Center for Information Security Services

The Congress and the Office of Management and Budget have enacted and published several Security and Information Assurance Requirements and Regulations. Follows are excerpts of several of the key documents:

Government Information Security Reform Act, P.L.106-398, Oct 2000

Requires annual agency program review, annual IG security evaluations, agency reporting to OMB, and an annual OMB report to Congress.
The Act became effective on November 29, 2000 and sunsets in two years.
The Act requires, for both *unclassified* and *national security* programs:

- Annual agency program reviews (generally CIO completes Self-Assessment Guide)
- Annual Inspector General (IG) evaluations
- Agency reporting to OMB the results of IG evaluations
- Annual OMB report to Congress summarizing the materials received from agencies
- Mandatory reporting of computer security incidents to FEDCIRC
- A plan for sharing information with FEDCIRC
- Agencies will submit this information beginning in 2001 as part of the budget.

Presidential Decision Directive (PDD-63)

Calls for a national effort to assure the security of increasingly vulnerable and interconnected public and private infrastructures of the United States by May 2003.

No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from today the United States shall have achieved and shall maintain the ability to protect the nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- The Federal Government to perform essential national security missions and to ensure the general public health and safety;
- State and local governments to maintain order and to deliver minimum essential public services.
- The private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

OMB Circular A-130

Requires a review of INFOSEC posture every 3 years. We recommend once per year or anytime significant System changes are made. At a minimum, agency programs shall include the following controls in their general support systems and major applications:

Controls for general support systems:

- Assign Responsibility for Security.
- Application Security Plan.
- Review of Security Controls.
- Authorize Processing. Use of the system shall be re-authorized at least every three years.

Controls for Major Applications:

- Assign Responsibility for Security. Assign responsibility for security of each major application to a management official knowledgeable in the nature of the information and process supported by the application and in the management, personnel, operational, and technical controls used to protect it.

- Application Security Plan. Plan for the adequate security of each major application, taking into account the security of all systems in which the application will operate.
    - Application Rules
    - Specialized Training
    - Personnel Security
    - Contingency Planning
    - Technical Controls
    - Information Sharing
    - Public Access Controls
- Review of Application Controls. Perform an independent review or audit of the security controls in each application at least every three years.
- Authorize Processing. Ensure that a management official authorizes in writing use of the application by confirming that its security plan as implemented adequately secures the application. The application must be authorized prior to operating and re-authorized at least every three years thereafter.

Government Paperwork Elimination Act, P.L.105-277, Oct 21,1998

An important tool to improve customer service and governmental efficiency through the use of information technology. This involves transacting business electronically with Federal agencies and widespread use of the Internet and its World Wide Web.

GPEA requires Federal agencies, by October 21, 2003, to:

- Allow individuals or entities that deal with the agencies the option to submit information or transact with the agency electronically, when practicable, and
- Maintain records electronically, when practicable
- Not deny legal effect, validity, or enforceability of electronic records and their related electronic signatures merely because they are in electronic form
- Encourages Federal government use of a range of electronic signature alternatives.

Information Technology Management Reform Act of 1996 (Clinger/Cohen Act)

In 1996, recognizing the importance of information technology for effective government, the Congress and President enacted the Information Technology Management Reform Act and the Federal Acquisition Reform Act. These two Acts together, known as the Clinger-Cohen Act, require the heads of Federal agencies to link IT investments to agency accomplishments, and establish a process to select, manage and control their IT investments. It links security to agency capital planning and budget processes, establishes agency Chief Information Officers, and re-codifies the Computer Security Act of 1987.

Under Title LI: Responsibility for Acquisitions of Information Technology
Subtitle C: Executive Agencies.

Requires the head of each executive agency to design and implement a process for maximizing the value and assessing and managing the risks of information technology acquisitions; to utilize the same performance- and results-based management practices as encouraged by the OMB Director; and to prepare an annual report to the Congress concerning progress in achieving such goals.

Computer Security Act of 1987, P.L. 100-235

The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use. Requires that each Federal agency identify Federal computer systems that contain sensitive unclassified information.

- The head of a Federal agency may employ standards for the cost-effective security and privacy of sensitive information in a Federal computer system.
- Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency.

Training shall be designed:

- To enhance employees' awareness of the threats to and vulnerability of computer systems; and
- To encourage the use of improved computer security practices.

- Regulations -- Regulations prescribing the procedures and scope of the training to be provided Federal civilian employees.
- Identification of Systems That Contain Sensitive Information -- Each Federal agency shall identify each Federal computer system, and system under development, which is within or under the supervision of that agency and which contains sensitive information.
- Security Plan -- Each such agency shall establish a plan for the security and privacy of each Federal computer system identified by that agency.

Now is the time for all Government agencies to act upon their overall Information Security posture. There are a host of programs and contracts established to do just that. Call your FTS Customer Service Representative (CSR) if you already have a relationship with FTS. If you are not currently a FTS customer or need additional information, please contact Peter P. Dauderis on 508-793-0202 or email him at peter.dauderis@gsa.gov. Peter can provide you with the information to get you started toward ensuring a healthy Information Security environment.

Here are two examples of current programs designed to assist agencies with their Information Security (IS)/Critical Infrastructure Protection (CIP) requirements:

ACES PROGRAM

Citizens have an important new tool to receive services, benefits and information directly from Federal Agencies.

The Government Paperwork Elimination Act (P.L. 105-277, Title XVII), allows citizens to use electronic technologies when filing information with, or retrieving it from the Federal Government. The Act, was signed into law October 1998, directs Federal agencies to provide public access to government services and documents by 2003 and give the public the option of submitting government forms electronically. Under GPEA, agencies will develop information systems that enable online submissions of forms, reports and other data. Agencies will be required to guard privacy and protect documents from being altered.

The FTS Access Certificates for Electronic Services (ACES) program facilitates secure on-line access to Government information and services by the Public through the use of public key infrastructure/digital signature technology.

If your agency interfaces with and exchanges information with the general public via the internet, i.e. any US Citizen, then ACES is for you. It clearly meets and exceeds all current requirements and standards for information exchange and digital signature over the internet.

SAFEGUARD PROGRAM

The FTS SAFEGUARD Program is a partnership consisting of the Federal Technology Service/Center for Information Security Services (CISS), the 27 BPA Industry Partners and the U.S. Government Agencies responsible for securing the Critical Infrastructure of the United States. FTS SAFEGUARD Program is a collective and collaborative effort culminating in a national organization structure based on infrastructure security awareness and education.
Whatever your particular agency needs are there is an Industry Partner poised to address your requirements.

Technology Update

A Fast Internet connection for all:

DSL[1] is here!

GSA has its Digital Subscriber Line (DSL) contract that brings fast Internet connections to far –flung offices.

Federal offices that rely on separate phone lines for voices and Internet-or a single line that requires them to use one service at a time-will get improved access at a faster speed under this contract from the General Service Administration's Federal Technology Service.

Officials also can order Digital Subscriber Line (DSL) technology via the Internet, according to the FTS official who spurred the drive to beef up access. DSL technology runs between the end user's location and the telephone switching stations. Although DSL runs over the existing copper lines that agencies now rely on, it will give users faster transmission speeds. DSL basically turns a single telephone line into two lines, telephone line into lines, with frequencies below 4 KHz reserved for voice and frequencies above that reserved for data. This enables users to access the Internet and transmit data even while they use the telephone for communications.

BellSouth, a provider of DSL, says users may access the Internet 30 to 100 times faster via DSL.

William Horst, Assistant Regional Administrator for FTS's New England office, envisions a Web portal where federal customers from Honolulu to Bangor, Maine, can order DSL with the click of a mouse. "To me, that's what will make this thing work," he said.

FTS, which packages contracts for the acquisition of telecommunications equipment and services for federal agencies, had

solicited contract bids to upgrade existing copper phone lines using DSL technology. Horst's office originated the idea and then passed it on to the agency's regional office in San Francisco, which has a larger staff and more experience in contracting.

"The California office will hammer out the contracts for purchasing DSL equipment and services and then turn them back to the New England division for administration", Horst said.

Ordering DSL, via a World Wide Web portal set up by the New England office is a snap, according to Horst.

The upgrade will give officials using old telephone wire systems high-speed Internet access and enable them to remain online without sacrificing voice telephone service.

"This may well be the answer for some of those [remote] offices. This could, in the long run, put them on the same level as their counterparts in the high risers, give them access at the same high speeds. The focus is to let all federal employment have the same access to the Internet." Horst said.

GSA announced the contract award on December 29, 2000. The contract period is January1.2001 through December 31.2001 with four one-year renewable options. Under the plan, the existing copper lines that link government user locations to telephone switching network will be modified to enable packed data to travel over the lines. While existing copper lines typically afford users a transmission speed of about 52 kilobits/sec, DSL provides a wide range of speeds. Bell South offers speeds ranging from 768-kilobits/sec downstream and 512 kilobits/sec upstream to a combination of 4 megabits/sec to 6-megabits/sec downstream and 640 megabits/sec upstream, as an example.

"One of the greatest and most recognized benefits is the additional speed and access," said Bill Getch, a spokesman for Bell South. "For example, if you're going to download a 3.75M video clip-you may have a regular dial-up speed on your computer of about 28.8 [kilo-bits/sec]-it'll probably take you about 17or 18 minutes to download. With DSL, it will [take] about 20 seconds."

The contract has provisions for 'Technical Refreshment' during annual contract renewal in order to take advantage of industry advancements in technology over the previous year.

For all the particulars go to Region 1 Web Page at:

http://r1.1k.gsa.gov/

CONTRACT REQUIREMENTS

The General Service Administration's contract for Digital Subscriber line technology included requirements for:

* ADSL and SDSL systems. ADSL, Asymmetric Digital Subscriber Line, Permits data to flow upstream and downstream over the line at different rates. SDSL, Symmetric DSL, enables data to flow at the same rate in either direction.
* Access speeds ranging from 144 kilobits/sec to faster megabit speeds. GSA is not setting a limit on the high speeds.
* A system that can be accessed by multiple users simultaneously.
* Flat fees vs. usage fees.